



Qualys Cloud Platform v2.x

Release Notes

Version 2.38

April 18, 2019

Here's what's new in Qualys Cloud Suite 2.38!

AV

AssetView

[Azure Instance State search token and Dynamic Tag Support](#)

SAQ

Security Assessment Questionnaire

[New Search Option for Template Selection](#)

WAS

Web Application Scanning

[Alert Conditions Revised For Multi-Scan](#)

[Cancel Scan Support for Child Scans](#)

MD

Malware Detection

[New Filters for Active and Inactive Schedules](#)

WAF

Web Application Firewall

[Enhancements to Events View](#)

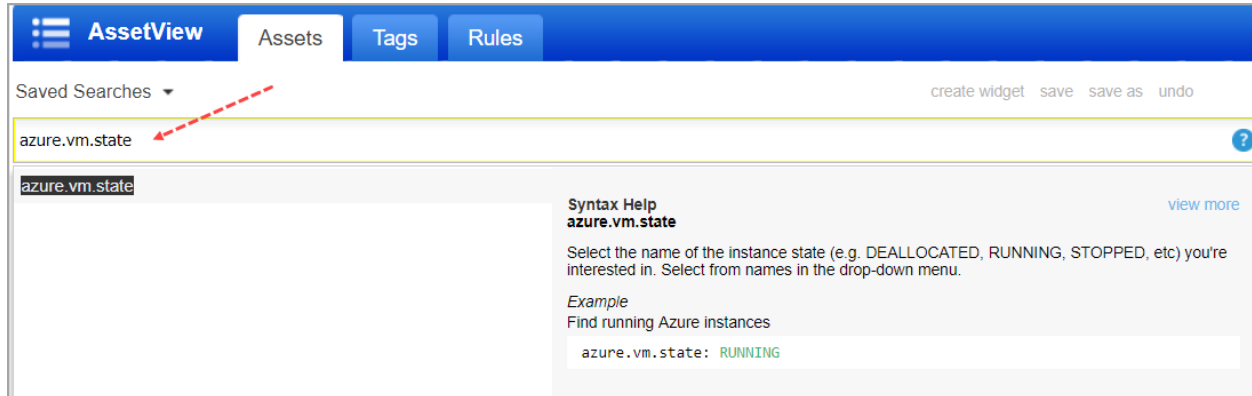
Qualys Cloud Platform

[App Picker has a new look!](#)

Qualys Cloud Platform 2.38 brings you many more Improvements and updates! [Learn more](#)

Azure Instance State search token and Dynamic Tag Support

AssetView now includes a new search token `azure.vm.state` for indexing the last state of Azure instances. Values can be: `STARTING`, `RUNNING`, `STOPPING`, `STOPPED`, `DEALLOCATED`, `DEALLOCATING`. This token can also be used for creating queries during Dynamic Tag Rule creation.

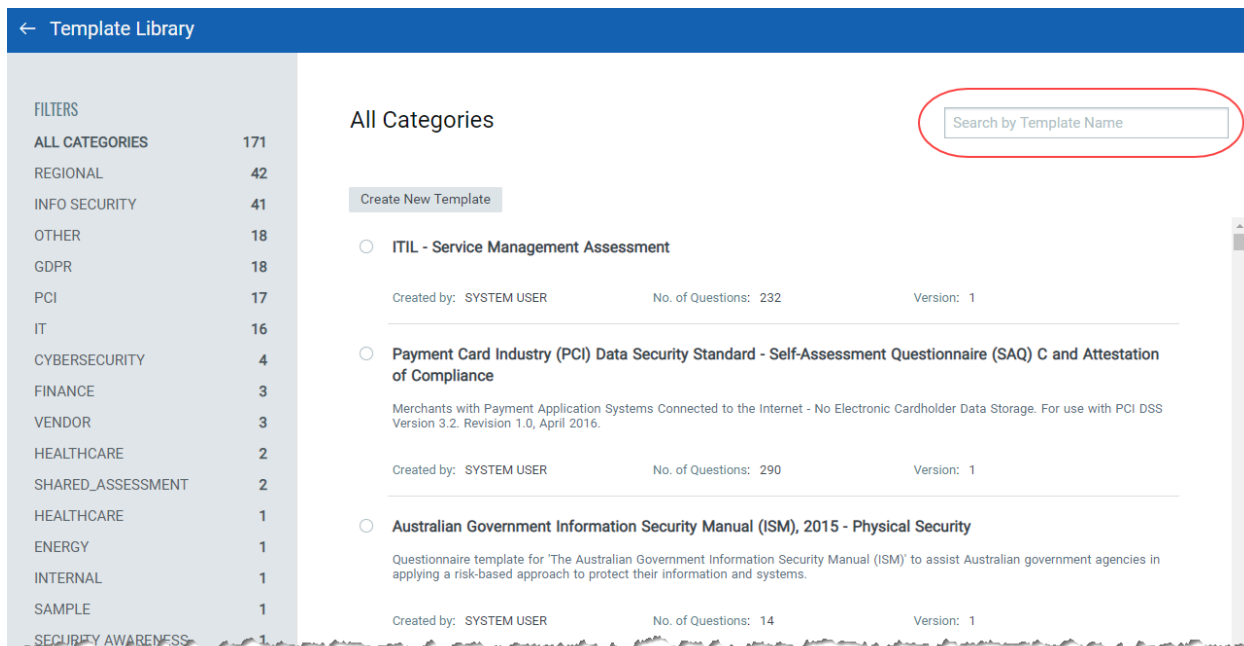


The screenshot shows the AssetView interface with a search bar containing the token `azure.vm.state`. A red dashed arrow points to this token. Below the search bar, a syntax help panel is displayed for `azure.vm.state`. The help text reads: "Select the name of the instance state (e.g. DEALLOCATED, RUNNING, STOPPED, etc) you're interested in. Select from names in the drop-down menu." An example query is shown: `azure.vm.state: RUNNING`.

New Search Option for Template Selection

You can now easily search for specific templates while creating or editing campaigns.

Simply navigate to the templates library and use the search bar to look up specific templates for your campaign.





The screenshot shows the 'Template Library' interface. On the left is a 'FILTERS' sidebar with a list of categories and their counts. The main area is titled 'All Categories' and features a search bar labeled 'Search by Template Name' (highlighted with a red circle). Below the search bar is a 'Create New Template' button. The main content area displays a list of templates, each with a radio button, a title, a description, and metadata (Created by, No. of Questions, Version).

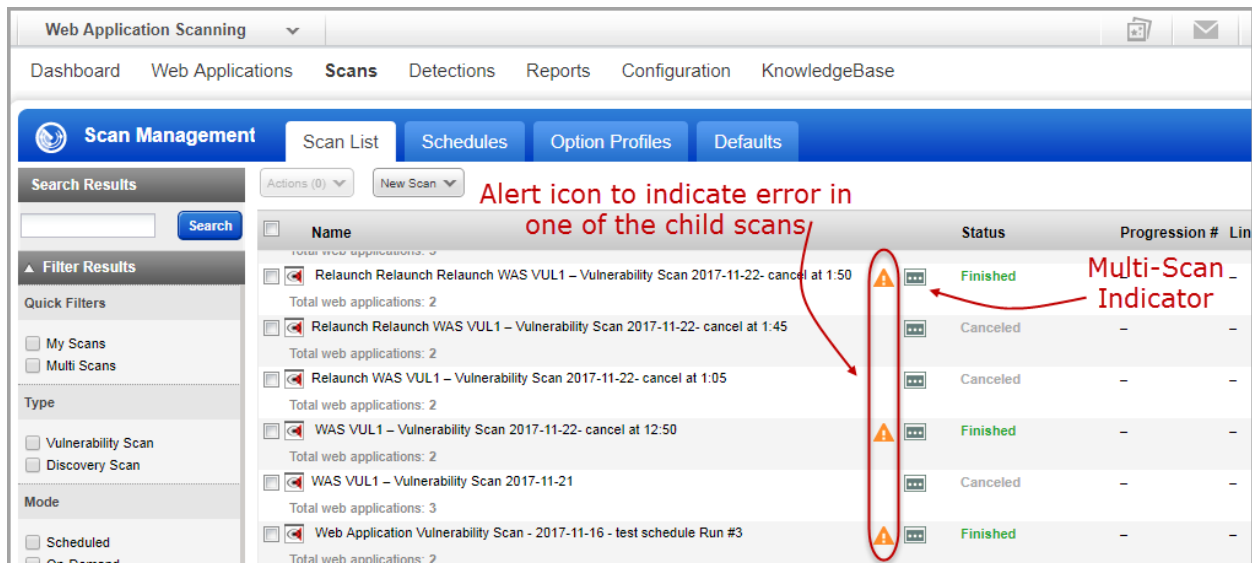
Category	Count
ALL CATEGORIES	171
REGIONAL	42
INFO SECURITY	41
OTHER	18
GDPR	18
PCI	17
IT	16
CYBERSECURITY	4
FINANCE	3
VENDOR	3
HEALTHCARE	2
SHARED_ASSESSMENT	2
HEALTHCARE	1
ENERGY	1
INTERNAL	1
SAMPLE	1
SECURITY AWARENESS	1

Template Name	Created by	No. of Questions	Version
<input type="radio"/> ITIL - Service Management Assessment	SYSTEM USER	232	1
<input type="radio"/> Payment Card Industry (PCI) Data Security Standard - Self-Assessment Questionnaire (SAQ) C and Attestation of Compliance	SYSTEM USER	290	1
<input type="radio"/> Australian Government Information Security Manual (ISM), 2015 - Physical Security	SYSTEM USER	14	1

Alert Conditions Revised For Multi-Scan

We now display alert icon for the condition where one or more scans within a multi-scan ends with "Service Errors Detected".

The  icon next to scan status to indicate that the current scan is a Multi-Scan. After the scan is completed, if you see , it indicates that the error in child scan and easily identify child scan failure in case of a Multi-Scan.



The screenshot shows the 'Scan Management' section of the Web Application Scanning interface. A table lists several scans with columns for Name, Status, and Progression #. A red circle highlights an alert icon (a triangle with an exclamation mark) next to the status 'Finished' for the scan 'Relaunch Relaunch Relaunch WAS VUL1 - Vulnerability Scan 2017-11-22- cancel at 1:50'. Red arrows point from text annotations to the alert icon and the 'Finished' status.

Name	Status	Progression #	Lin
Relaunch Relaunch Relaunch WAS VUL1 - Vulnerability Scan 2017-11-22- cancel at 1:50	Finished	-	-
Relaunch Relaunch WAS VUL1 - Vulnerability Scan 2017-11-22- cancel at 1:45	Canceled	-	-
Relaunch WAS VUL1 - Vulnerability Scan 2017-11-22- cancel at 1:05	Canceled	-	-
WAS VUL1 - Vulnerability Scan 2017-11-22- cancel at 12:50	Finished	-	-
WAS VUL1 - Vulnerability Scan 2017-11-21	Canceled	-	-
Web Application Vulnerability Scan - 2017-11-16 - test schedule Run #3	Finished	-	-

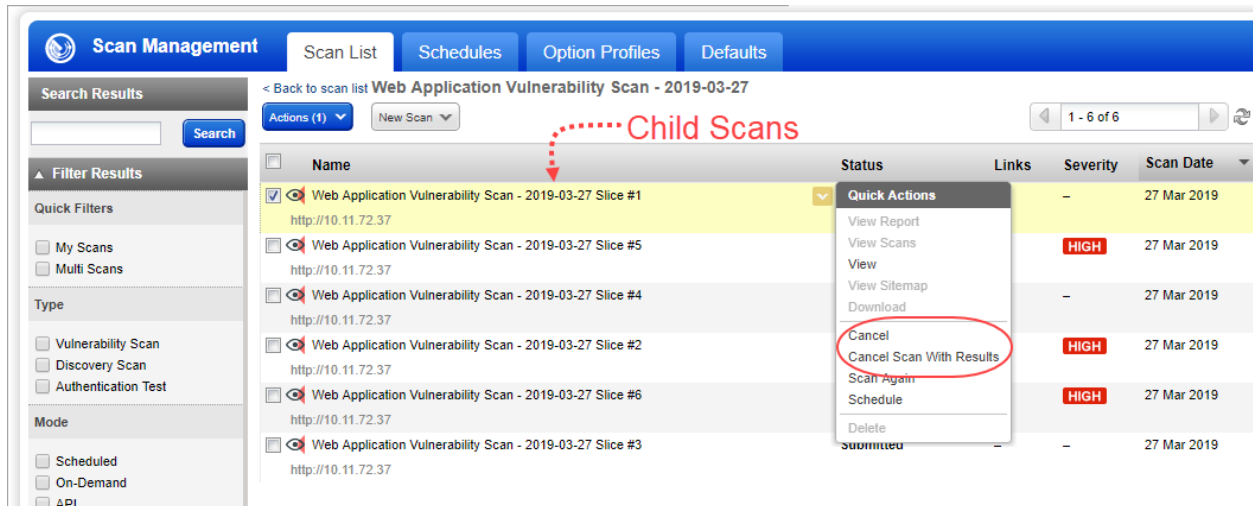
The alert icon is displayed for following conditions:

- one or more scans within a multi-scan ends with "Service Errors Detected".
- if any of the child scans ends with "Error" scan status.
- if none of the child scans end with "Finished" status
- if all slices that are having either of below mentioned statuses: No Host Alive, No Web Service, Time Limit Reached (Green color), Scan Not Launched, Scanner Not Available.
- if the multi-scan reached the designated cancel time but there were still child scans in "submitted" status. When this occurs, the slices in submitted status have final status of "Time Limit Reached" in orange color.

Note: The alert icon is NOT shown if one or more scans within a multi-scan ends with "Canceled" or "Canceled with Results".

Cancel Scan Support for Child Scans

You can now cancel an unfinished child scan in a multi-scan. Just select the scan in the scans list and choose Cancel or Cancel Scan with Results from the quick action menu.



The screenshot displays the 'Scan Management' interface. The main content area shows a table of scans under the heading 'Web Application Vulnerability Scan - 2019-03-27'. A red dashed arrow points to the first scan, 'Web Application Vulnerability Scan - 2019-03-27 Slice #1', which is highlighted in yellow and labeled as a 'Child Scan'. A context menu is open over this scan, showing options: View Report, View Scans, View, View Sitemap, Download, Cancel, Cancel Scan With Results (circled in red), Scan Again, Schedule, and Delete. The table columns are Name, Status, Links, Severity, and Scan Date. The first scan has a status of 'Submitted' and a severity of '-'. The other scans have a status of 'Running' and a severity of 'HIGH'.

Name	Status	Links	Severity	Scan Date
Web Application Vulnerability Scan - 2019-03-27 Slice #1 http://10.11.72.37	Submitted		-	27 Mar 2019
Web Application Vulnerability Scan - 2019-03-27 Slice #5 http://10.11.72.37	Running		HIGH	27 Mar 2019
Web Application Vulnerability Scan - 2019-03-27 Slice #4 http://10.11.72.37	Running		-	27 Mar 2019
Web Application Vulnerability Scan - 2019-03-27 Slice #2 http://10.11.72.37	Running		HIGH	27 Mar 2019
Web Application Vulnerability Scan - 2019-03-27 Slice #6 http://10.11.72.37	Running		HIGH	27 Mar 2019
Web Application Vulnerability Scan - 2019-03-27 Slice #3 http://10.11.72.37	Running		-	27 Mar 2019

- Cancel: Choose the Scan Cancel option to automatically cancel a scan after some period of time a number of hours, or at a specific time. You can choose the Cancel Option for a new scan, multi-scan, child scan and a scan schedule, and for a web application's default scan settings.

- Cancel Scan with Results: The Cancel Scan with Results option is now available for child scan in a multi-scan. You could also use Cancel Scan with Results option from the quick action menu to cancel an unfinished scan and then retrieve the partial scan results.

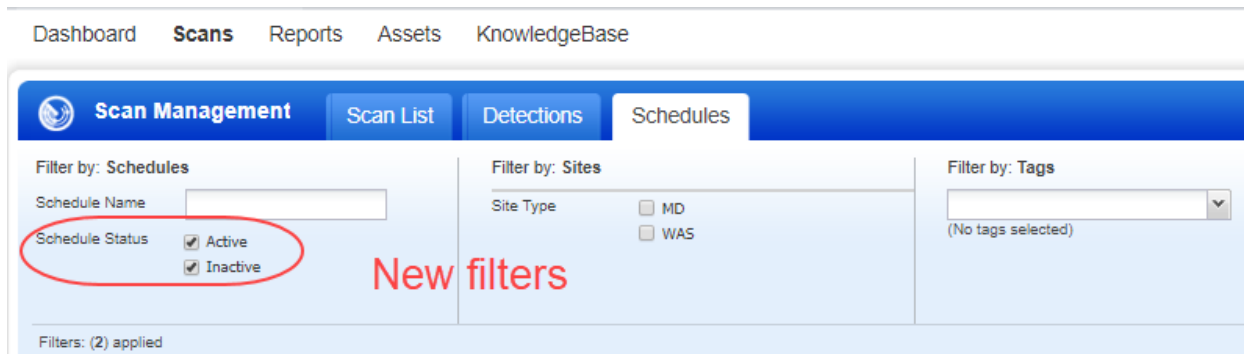
Note: The Cancel option or the Cancel Scan with Results option is enabled only after 20 minutes of scan goes into Running status.

To view the partial data that has been retrieved by the unfinished scan, click View Report from the quick actions menu for scans with Canceled With Results status.

New Filters for Active and Inactive Schedules

We have now introduced two new filters for schedule status that will help you narrow down your search results: Active and Inactive.

Go to Scans > Schedules and click Show Filters. The new filters appear under Schedule Status.

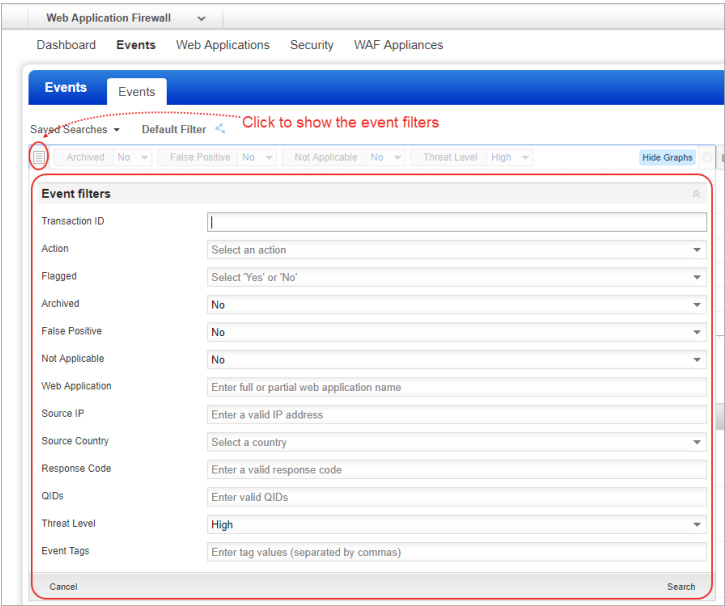


Active: Selecting this option will display all schedules that are currently active.

Inactive: Selecting this option displays all schedules that are deactivated.

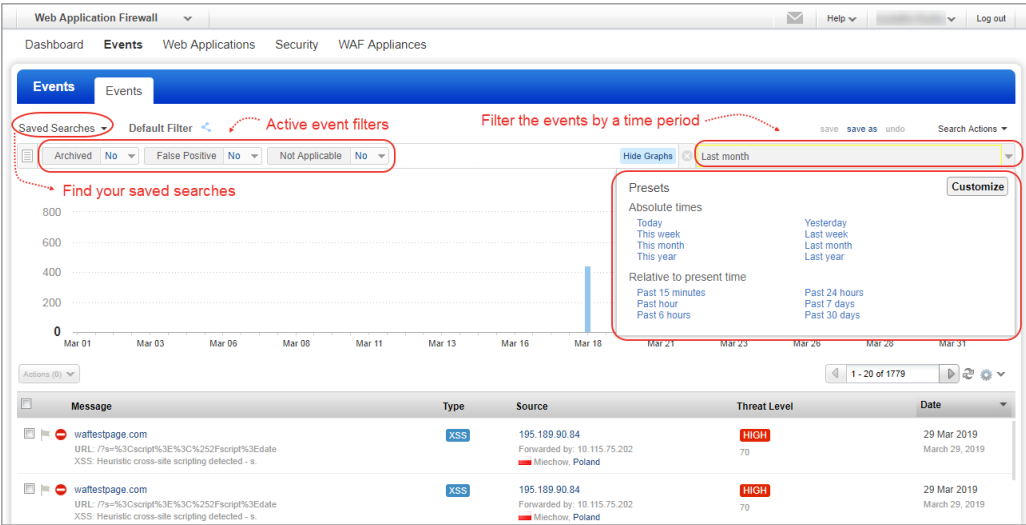
Enhancements to Events View

We have enhanced the events view to help you quickly find the events using the event filters. New Event tab has three sections: The top section has an event filters icon. Click the icon to view and choose filters to search for events.



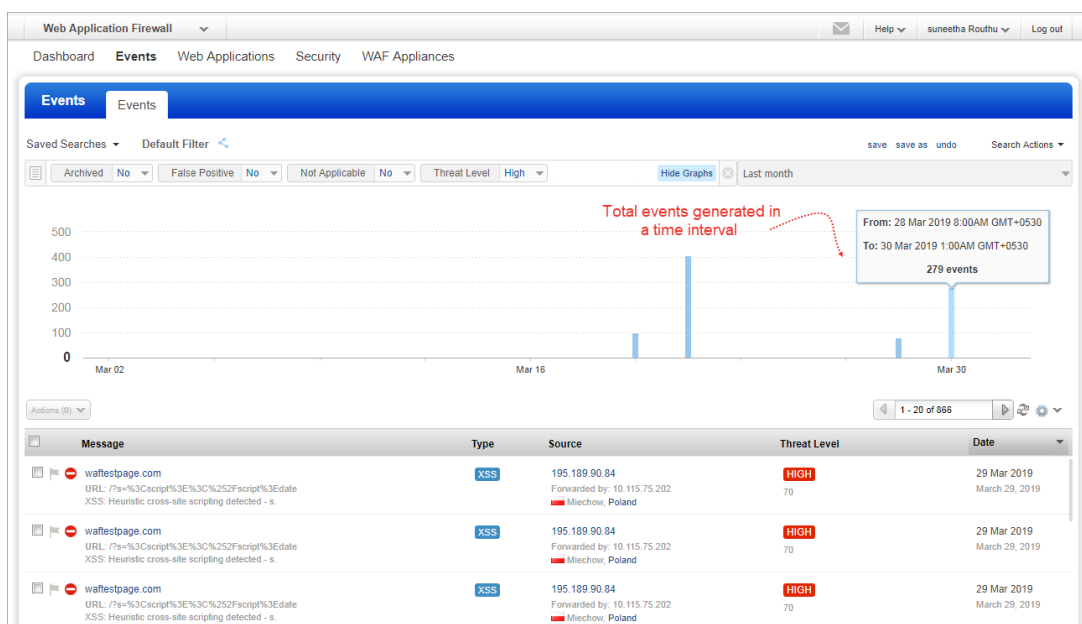
You can see the chosen event filters with their values in a search box. You can set new values for these filters. Any new filter chosen will appear in the search box.

You have an option to filter your events by date, time and year. You can view events either for a preset period or specify a range using date time pickers available in the customize option. You can group your event filters and create new searches using the “save as” option. You will find your searches in Saved Searches.



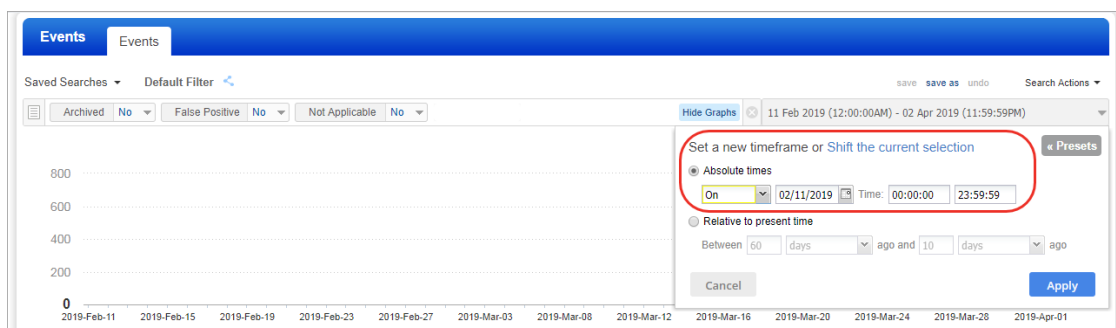
The middle section shows the search results to give a graphical break up of events generated at different time periods. The time period can be hourly, monthly or yearly depending on the date time filter that you selected. Move your mouse over an event bar to view the date and time of the generated events and a total count of events for that period.

At the bottom of the page, we show the search results based on the applied event filters. Here you can view the events and their details generated for your web applications. Events list and event details are now shown in the same Events tab. Click “Back to list” to go back to the events list.

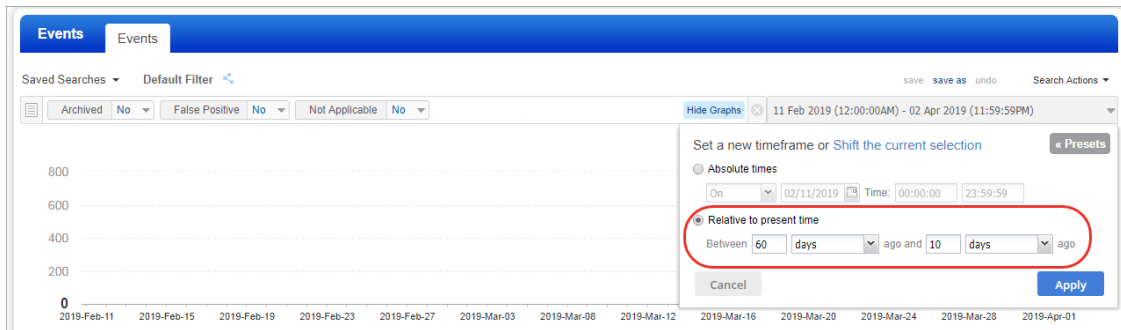


Customize your time period for your events search

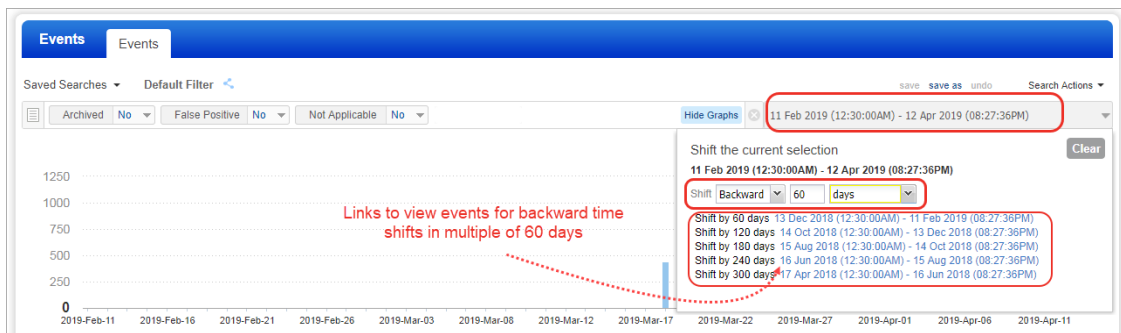
You can customize presets for Absolute times and Relative to present time. Customize “Absolute times” option to view all the events generated on or before a particular date and time, from a particular date and time or between two time periods.



Customize “Relative to present time option” to view all the events generated from a specified time till the current time. You can specify a range here to see events generated between two time periods ago calculated from the current time period. For example: you can form a range to view all the events generated between a date 60 days ago from the current date and 10 days ago from the current date.

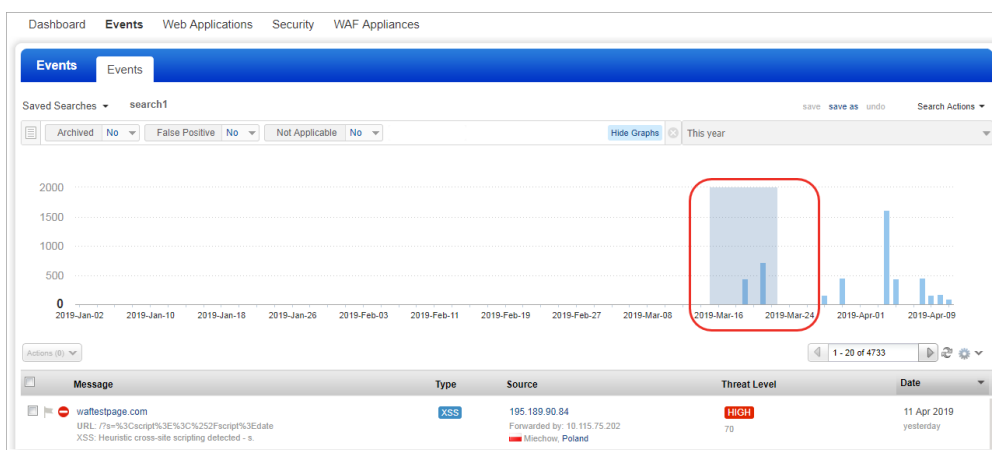


You can use the “Shift the current selection” option to shift the selected time period backward or forward by a specified duration. Based on your selection, we will calculate backward or forward time periods and show you five shift durations in multiples of the selected time period with links that you can click to view events generated during that time period.

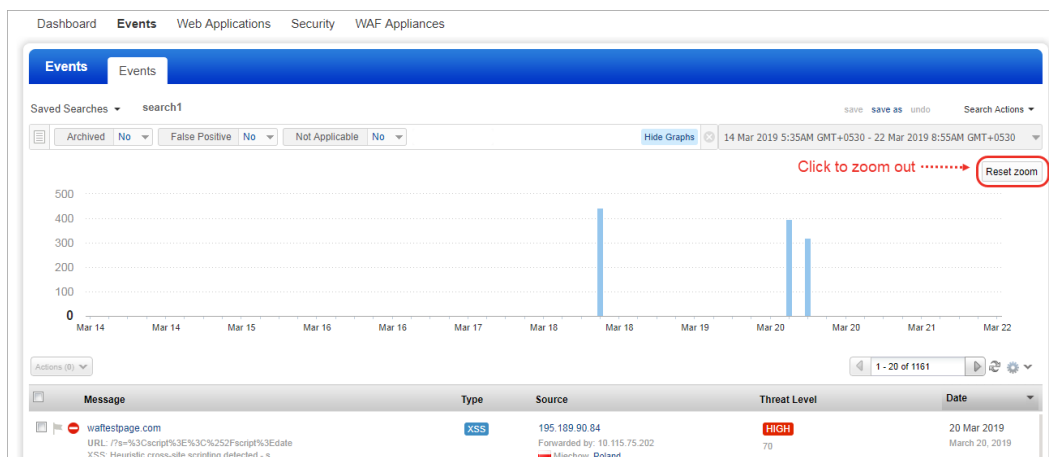


Zoom in and out graphical event data

We have also provided a zoom in option to filter your event data to give you a further break up of the events generated during a time period. For example, if the graphical data shows events generated during a year, then zooming over a time period will filter event data to show you more accurate analysis of events generated for that period. You can zoom in only one level of event data. To zoom in, click and drag your mouse pointer over one or more event bars or just click a single event bar



Use Reset zoom to go back to the original view.



Find QIDs responsible for triggering the event

Now, for events with multiple QIDs, we will help you identify the QIDs for which the event is triggered. In Events View mode, select the QIDs one by one to see the request getting highlighted for QIDs that have triggered the event. If a QID did not trigger the event, the request is not highlighted for that QID.

The screenshot shows the 'Events' view for a specific event. The event details section includes a table of detections. A red arrow points to the first row of the table, which is circled in red. Below the table is a 'Request' section with a red circle highlighting the request log.

Detections	QID	Type	Confidence	Threat Level
XMLi: 1 XML tags detected.	226018	-	40%	MED 40
XSS: Heuristic cross-site scripting detected - s.	150001	XSS	80%	HIGH 70
XSS: Script tag detected - <script <%2fscript-date	150001	XSS	40%	MED 40
XSS: HTML tag detected - <script .	150001	XSS	40%	LOW 30
RCE: Exact command detected - date.	226008	-	50%	MED 40
Detected: XMLi, XSS, CommandExec.	-	-	80%	HIGH 70

```
GET /?s=%3Cscript%3E%3C%252Fscript%3Edate HTTP/1.1
User-Agent: curl/7.39.0
Host: wafestpage.com
Accept: */*
Accept-Encoding: gzip, deflate, sdch
```

Qualys Cloud Platform

App Picker has a new look!

The apps in your subscription are now grouped in the app picker making them easier to find. A sample app picker is shown to the right.

Apps will be grouped into these categories:

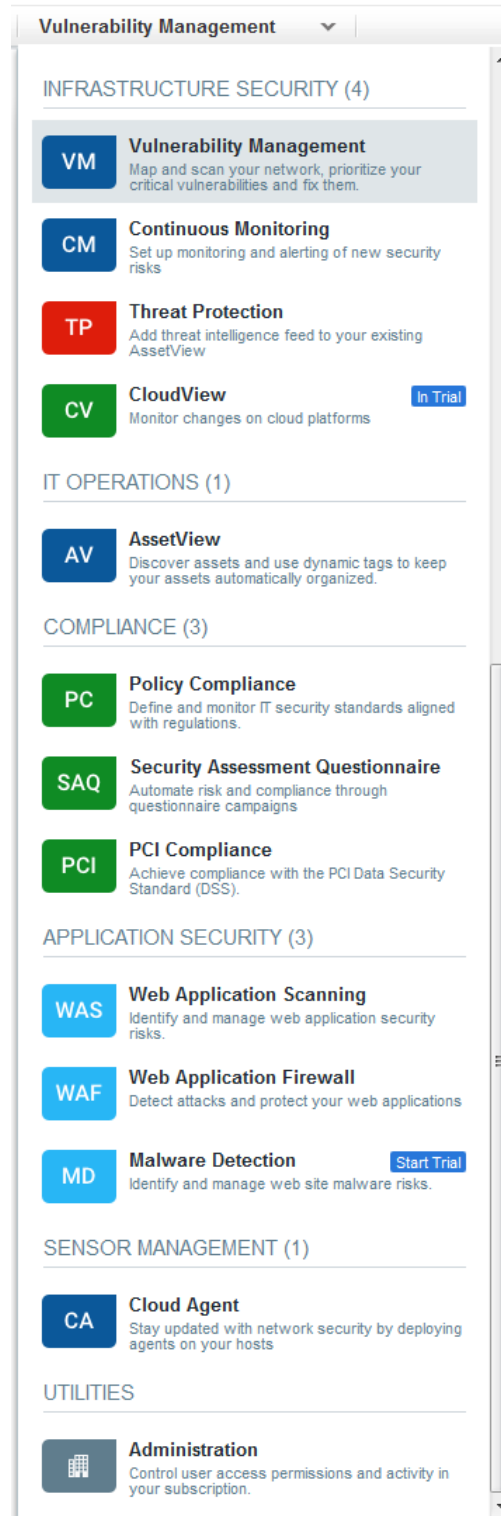
- Infrastructure Security
- IT Operations
- Security Operations
- Compliance
- Application Security
- Sensor Management
- Utilities

In Trial

Indicates that you currently have a trial version of the app.

Start Trial

Indicates that a trial version is available if you want to try the app.



Issues addressed in this release

Qualys Cloud Platform 2.38 brings you many more improvements and updates.

AV

AssetView

TP

ThreatPROTECT

- Fixed an issue in AssetView, where incorrect data was displayed while searching for assets using the vulnerability published date.
- Fixed an issue where the dynamic tag for aws.ec2.instanceState was not getting evaluated and applied to assets upon state change.
- Fixed an issue where Asset Details displayed incorrect Last Checked-In date.
- The location map in Asset Details is now improved to make it look better.
- Fixed an issue in Asset Details, where data was intermittently disappearing from the Patch Management tab.

CA

Cloud Agent

- Fixed an issue in Cloud Agent, where the "Getting Started" page was displayed for users with activated agents and scan data. Now the "Getting Started" page will be displayed only to users that do not have any activated agents or scan data.
- Previously, in the CloudAgent API call, providing nested elements for agentInfo in the "fields" parameter (e.g., fields=agentInfo.manifestVersion.vm) did not work unless you also provide an additional element such as ID, created, updated, etc of the record you are searching for (e.g., fields=id,agentInfo.manifestVersion.vm). This is fixed and now you need not provide the additional element.

CS

Container Security

- In Container Security the Container Events and Total Events widgets are no longer available on the dashboard, and the word "rogue" is changed to "drift" in the search tokens and on the UI.

SAQ

Security Assessment Questionnaire

- While creating or editing answer settings in a template, we have changed the label "Select Score" to "Risk Score" for better readability.
- We fixed an issue in the Delegate Section workflow where the user's list disappeared when typing a name.

WAS**Web Application Scanning**

- Now you can contact Qualys Support or your Technical Account Manager to change the report download URL that appears in the WAS scan completion email for your subscription.
- We have now rectified the behavior to consistently display the scan report when opened from Scan results email link. Earlier, on some occurrences, the dashboard was displayed.
- We have now updated the Finding API XSD to include PROTECTED as one of the status parameter options and removed the invalid status options.
- User will now receive only one email notification once the scheduled report generation is completed. Earlier, users received multiple email notifications.
- We have now fixed an issue for downloaded Web Application report and Scan report in HTML format where forward slashes in HTML reports will now be displayed correctly.
- Fixed issue regarding unwanted delete of tags from WAS scheduled scans (mysterious deactivation of schedules)
- In case of multi-scan, users will now receive an email notification after every child scan completion along with an email after Parent-scan completion.
- We have rectified the WAS API User Guide to include all the detection categories supported for Finding API.
- We have improved the description in WAS Online help for FAQ related to Detection scope.

WAF**Web Application Firewall**

- Now the user can view detailed configurations for Built-in Policy Templates including the sensitivity rating for the various detection categories in the Application Security tab.
- We have enforced the rules for specifying MIME types in the "Content-Type" header as per the RFC standards. Follow the RFC standards to define MIME types when you choose "Deny All, but Explicitly Allow" option to specify the allowed content types in the Request Content-Type section in the HTTP Protocol tab during the HTTP Profile create or update.
- We have fixed an issue where, in the web application edit mode, the SSL certificate in the Application tab for the Web application was not getting populated. The issue was observed when the primary URL had HTTP and the secondary URL had HTTPS URL. This issue is fixed now.
- We have fixed an issue where when viewing a security policy, the "Blocking" label shown in Thresholds in the Policy Controls tab was overlapping the threshold value for the "Logging" label. Now you can move your mouse pointer over the "Logging" label to view its thresholds value.

- We have fixed discrepancy issues and the Published date is now displayed accurately in the Dashboard. In case a published date is not available then the inserted date is displayed as Published date.
- Accurate values are now displayed in the dashboard widgets even after applying the filters.
- Vulnerability severity is now accurately displayed in the Vulnerabilities tab and on the Summary page of Vulnerability details
- Token help is now displayed accurately and consistently on the Vulnerabilities tab.
- Token help is now displayed accurately while editing a dashboard widget.
- The token vulnerabilities.vulnerability.exploitability has been removed.
- The Dashboard widget: GroupBy now displays accurate results.
- Widgets are now rendered accurately even when you toggle between between widgets while editing.
- IP address is now displayed correctly in the Vulnerabilities tab, Asset Details page, and Location maps.
- OS name and icon is now displaying properly on the Vulnerability Details page and the Asset details page.